IN GROUPE DENMARK PS

Remote QSCD PS

Document information			
No. of pages : 15	Reference : rQSCD PS	Department : eID Application Development	Classification : Public
Creation date : 17/02/2025		Last saved update: February 25	Version : 1.0

Version history			
Version	Date	Author	Description of update Updated paragraphs
1.0	17/02/2025 00:00	KJAERSGAARD, Jan	Initial version
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		
	Cliquez ou appuyez ici pour entrer une date.		

CONTENTS

1 INTRODUCTION

IN Groupe Denmark A/S is a qualified trust service provider under the eIDAS regulation. Its services cover certificate issuance, time-stamp issuance and signature generation.

IN Groupe Denmark A/S is denoted QTSP in this document.

This document is the practice statement for management of remote qualified signature creation devices, which is a qualified service offered by the QTSP.

The QTSP documentation is organised with a generation practice statement document describing how requirements from **Error! Reference source not found.** are met, and this document references to the general description for relevant topics.

The service is part of a public key infrastructure, that also includes certification and time-stamp authorities. ¨

2 DEFINITIONS AND ABBREVIATIONS

Term	Definition
CA	Certification Authority
CPS	Certificate Practice Statement
QTSP	Qualified Trust Service Provider
QSCD	Qualified Signature Creation Device
rQSCD PS	Remote Qualified Signature Creation Device Practice Statement
SAD	Signature Activation Data
SAP	Signature Activation Protocol
SAM	Signature Activation Module
eID	Electronic Identification Data
RA	Registration Authority
DTBS/R	Data To Be Signed/Representation
UTC	Coordinated Universal Time
SIEM	Security Information and Event Management
SSAS	Server Signing Application Service

3 GENERAL PROVISIONS ON PRACTICE STATEMENT AND POLICIES

3.1Practice Statement Requirements

The QTSP has described general consideration related to practice statements in [TSP PS].

The TSP use cryptographic modules for subject key pair generation and signature creation. The module uses recommended and certified cryptographic algorithms.

The qualified signature creation device used by the QTSP uses a Signature Activation Module conformant to [EN 419 241-2] using a cryptographic module conformant to [EN 419 221-5].The operation of the QSCD meets the requirement stated in the manufacturers documentation, the certifications do not pose additional requirements.

3.2SCP Name and Identification

The QTSP conforms to the policy, [TS 119 431-1], EU SSAS policy identified by:

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd-v2 (4)

3.3Participants

The participants in the QTSP services are described in [CPS].

4 TRUST SERVICE PROVIDER PRACTICE

4.1Publication and Repository Responsibilities

The QTSP publication and repository is described in [CPS].

4.2Signing Key Initialization

4.2.1 Signing Key Generation

The [CPS] describes the remote qualified signature creation device, which generates subject keys. The keys are created using cryptographic algorithms suitable for the life-time of the certificate associated to the private key.

The remote qualified signature creation device is only used for the signature service to generate and use signature keys.

All private and secret keys used by the QTSP are only used for their intended purpose and not shared. Controls are in place for all keys to ensure that access to the key is restricted to the intended system or role for the specific purpose.

Infrastructure keys are automatically updated and distributed they are securely protected.

If any keys used by the QTSP is suspected of compromise or the algorithm not considered usable for the purpose, the key is updated.

4.2.2 eID Means Linking or identity linking

Subject keys are one-time signing keys and are linked to the subject identity.

Subject enrolment is described in [CPS].

4.2.3 Certificate Linking

During a signing session, the QTSP generates a subject key pair is generated and issues certificate for the public key. The private key and certificate and linked together by the signing session.

Since the certificate is issued during the signing session, the private key cannot be used before the certificate is issued.

4.2.4 eID Means Provision

N/A. The QTSP does not provide an eID mean.

4.3Signing Key Life-cycle Operational Requirements

4.3.1 Signature Activation

During a signing session, the QTSP directs the subject to a RA to ensure the subject is identified or authenticated. This is carried out before the subject key pair is generated.

The QTSP uses an RA with an electronic identification scheme, the QTSP requires that the electronic identification scheme meets the applicable requirement in the implementing act [2015/1502] for level of assurance high. In particular, the authentication mechanism prevents a malicious user to use subject authentication credentials, which do not belong to him/her.

The subject does not have access to any sensitive system objects at the QTSP. The subject is directed to the RA and based on information received from the RA, the QTSP performs the steps of the signature activation protocol to sign the document as authorized by the subject. The QTSP completes the signature creation within a few seconds after receiving the information from the RA. Since signature keys are created, assigned to the user and certified during the signature flow, the link between the user and signature key is bound to the session. Signature keys are created during the flow and only used when assigned to a user.

During the signature protocol, a SAD is generated under the users control and presented for the SAM. The SAD explicitly describes which DTBS/R that can be signed by the user's signature key. The QTSP issues the SAD based on user information received by direct interaction with the RA.

In addition to security controls for the authentication mechanism, the SAP has been designed such that the SAD is only available within the QTSP environment using interfaces solely available for the QTSP.

The QTSP always issues short-term certificates during a signing session, to ensure that the certificate is valid at the time of signing.

During the signing session, the user actively consents to the signature operation by

1) Accepting the Terms and Conditions and is prompted to accept the T&C for using the trust service, and
2) Clicks on the Sign button.

The issuance of SAD is always carried out by the QTSP during a signing session, when the subject identity has been established through an authentication or identity verification process meeting the requirements in [2015/1502] for level of assurance high, and the subject has consented to the signature operation, and subject attributes has been received from the RA.

The SAD is generated by the QTSP and never leaves the QTSP environment. It is passed to the Signature Activation Module using the Signature Activation Protocol. Once the SAD reaches the SAM, it is verified to in integrity, and it is checked to contain the expected records including subject information, digests to be signed and reference to the signature key. Since a signature key is always created during a signature flow, it is automatically linked to the specific user, SAP and SAD.

4.3.2 Signature Key Deletion

Signature keys are generated and automatically destroyed during a signing session. Signature keys are not backed-up.

4.3.3 Signature Key Backup and Recovery

The QTSP does not create backup of signature keys.

4.4Facility, Management, and Operational Controls

4.4.1 General

See [TSP PS].

4.4.2 Physical Security Controls

See [TSP PS].

4.4.3 Procedural Controls

See [TSP PS].

4.4.4 Personnel Controls

See [TSP PS].

4.4.5 Audit Logging Procedures

See [TSP PS] for general considerations related to collection of evidence.

The signature service maintains an audit log, which includes records of critical system events. The audit records are protected in integrity and records can only be added to the audit log. The integrity of the audit log can be verified.

Access to the audit record is only granted to authorized individuals with a role permitting it.

Each audit record includes the time at which the event was noticed. The time used by the QTSP services is synchronized with UTC.

The audit record contains information on time, type and description of the event including, where relevant the subject it relates to.

The platform provider includes a SIEM service which ensures that all security events are logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and SSAS system access attempts.

The audit log contains personal data related to certificate issuance. The audit log or archive do not contain any signing keys.

In case the system can not create an event for the audit log, the session will terminate with an error.

4.4.6 Records Archival

See [TSP PS].

4.4.7 Key Changeover

No policy requirement.

4.4.8 Compromise and Disaster Recovery

See [TSP PS].

4.4.9 SSASP Service Termination

See [TSP PS].

4.5Technical Security Controls

4.5.1 Systems and Security Management

The QTSP uses a system for remote signing, which supports roles with different privileges.

Security officers do not carry out any operation on the system but supervises the overall security and participates as observer for operations, which are security critical. The actual execution of security critical operations is carried out by system administrator supervised by a security officer.

System operators and administrators are carried out by the same personnel. A security officer cannot take the role as a system operator or system auditor.

A system operator can only perform administrative tasks and not perform, in that role, any other operations. And similarly, a user authenticated by the RA, cannot carry out any other operation than signing.

Only users who has been authorized to assume the role of Security Officers or System Auditor can assumes these roles.

All privileged users are named and have the required qualification to assume that role.

It is only privileged users that has access to the system.

During the signature flow, as part of the signature flow, the SCA instructs the SSA to:

- Create a user key pair using the rQSCD
- Certify the key pair by reaching out the the CA
- Persist the issued certificate at the rQSCD
- Sign the supplied DTBS/R

Access to the system for users, which are not a signer, is carried out through dedicated equipment and protected by the access control management system using strong authentication. If a user enters incorrect authentication credentials too many times, the user's access is suspended. The system requires that the user provides authentication credentials after a log-out or if the session was left idle.

4.5.2 Systems and Operations

The rQSCD manufacturer has provided extensive documentation with instructions on installation and operation of the system. In addition, the software is deployed in an environment, which is physically protected with extensive access control, which ensures the integrity of the system is maintained.

The supplied documentation describes how privileged roles are configured and supported by the system and the QTSP has mapped this into its own processes.

The system receives accurate time source linked to UTC through the same scheme as the QTSPs qualified time-stamping service.

4.5.3 Computer Security Controls

See [TSP PS].

4.5.4 Life Cycle Security Controls

See [TSP PS].

4.5.5 Network Security Controls

See [TSP PS].

4.6Compliance Audit and Other Assessments

The used policy does not provide any requirements. See [[TSP PS] for details.

4.7Other Business and Legal Matters

4.7.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP's services.

4.7.2 Financial Responsibility

The used policy does not provide any requirements.

4.7.3 Confidentiality of Business Information

The used policy does not provide any requirements.

4.7.4 Privacy of Personal Information

See [TSP PS].

4.7.5 Intellectual Property Rights

The used policy does not provide any requirements.

4.7.6 Representation and Warranties

The used policy does not provide any requirements.

4.7.7 Disclaimer of Warranties

See clause 6.7.6.

4.7.8 Limitations of Liability

Limitations on liability are covered in the terms and conditions as per clause 6.8.4.

4.7.9 Indemnities

The used policy does not provide any requirements.

4.7.10 Term and Termination

See [TSP PS].

4.7.11 Individual Notices and Communications with Participants

The used policy does not provide any requirements.

4.7.12 Amendments

The used policy does not provide any requirements.

4.7.13 Dispute Resolution Procedures

See [TSP PS].

4.7.14 Governing Law

See [TSP PS].

4.7.15 Compliance with Applicable Law

See [TSP PS].

4.7.16 Miscellaneous Provisions

No policy requirement.

4.8Other Provisions

4.8.1 Organizational

See [TSP PS].

4.8.2 Additional Testing

No policy requirement.

4.8.3 Disabilities

See [TSP PS].

4.8.4 Terms and Conditions

See [TSP PS].

5 FRAMEWORK FOR DEFINITION OF SERVER SIGNING APPLICATION SERVICE POLICY BUILDT ON THE PRESENT DOCUMENT

The QTSP uses the signature service policy found in [TS 119 431-1].

6 REFERENCES

References	
Text reference	**Description**
[EN 319 401]	ETSI EN 319 401, Electronic Signatures and Trust Infrastructures (ESI); General Policy Requirements for Trust Service Providers, v3.1.1
[CPS]	Certification Practice Statement, IN Groupe Denmark A/S, 2025.
[TSP PS]	Trust Service Provider Practice Statement, IN Groupe Denmark A/S, 2025.
[TS 119 431-1]	ETSI TS 119 431-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
[EN 419 241-1]	CEN EN 419 241-1, CEN TC224 WG17, Trustworthy Systems Supporting Server Signing – Part 1: General System Security Requirements, 2018.
[EN 419 241-2]	CEN EN 419 241-1, CEN TC224 WG17, Trustworthy Systems Supporting Server Signing – Part 2: Protection profile for QSCD for Server Signing, 2019.
[EN 419 221-5]	CEN EN 419 221-5, CEN TC224 WG17, Protection profiles for TSP Cryptographic modules - Part 5 Cryptographic Module for Trust Services, 2016.
[2015/1502]	COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.